

[0088] After the completion of the authentication cancel confirmation, the client service provider requests the IP server to start a user cancel processing CGI. In response, the IP server executes the cancel processing (namely the deletion of the registration) for the user (S131). Then, the IP server sends an acknowledgement response to the client service provider.

[0089] In response, the client service provider deletes the site ID of the IP site registered in relation with the flash ID of that user from the My Menu DB 414a (S124).

[0090] Subsequently, the client service provider sends an HTML text to the terminal browser for notifying it of the completion of the deletion (S114).

[0091] The flash ID may be encrypted by use of various encryption algorithms. The present embodiment uses SSL (Secure Socket Layer), which is a typical encryption algorithm for use between a Web server and a Web browser.

[0092] Referring to FIG. 19, there is shown the processing flows of the terminal browser and the client service provider in authenticating the client service provider by the browser and sending encrypted data from the browser to the client service provider. First, the browser sends a request for connection to the server (S211). Receiving this request (S221), the server sends its server certificate to the browser (S222). This certificate is issued by a certificate authority which manages the public key of the user (in this example, the client service provider). The server certificate contains the public key of the server, the expiration date of the certificate, the serial number allocated by the authority, the name of the authority, and a digital signature. The digital signature is generated by encrypting a hash value having contents of a certificate by the private key of the certificate authority for tamper prevention. The browser incorporates the public keys of main certificate authorities and decodes the digital signature by use of the corresponding public key to verify the identity of the server. Namely, the public key encryption system is used to verify, by the user, that a particular Web server is an appropriate one. Thus, the browser authenticates the server (S213). Then, the browser generates a secret key (based on the common key encryption system) for this session (S214), encrypts the generated secret key by the public key of the server, and sends the encrypted secret key to the server (S215). Further, by use of this secret key, the browser encrypts the data to be encrypted and sends the encrypted data to the server (S216). Upon reception of the encrypted data (S224), the server decrypts the encrypted data by the secret key (S225). Namely, for actual data transfer operations, the secret key encryption system faster in encryption and decryption processing than other encryption system is used.

[0093] The above-mentioned processing also holds with the transmission of the flash ID from the client service provider to a content provider in an encrypted manner.

[0094] In the above-mentioned first embodiment, the mobile information terminal accesses the Internet through a communication device externally connected to the mobile information terminal. If the mobile information terminal incorporates communication capabilities, such an external communication device need not be connected. The present invention is also applicable to camera-equipped digital mobile phones compliant with IMT-2000 such as W-CDMA

for example. The following describes such a camera-equipped digital mobile phone practiced as a second embodiment of the invention.

[0095] Referring to FIG. 20, there is shown an overall configuration of a networks system which uses the above-mentioned digital mobile phones. In FIG. 20, reference numeral 200 denotes the network system to which mobile phones MS3 and MS4 are connected. Base stations CS1 through CS4, stationary wireless stations, are each arranged in each of cells obtained by dividing a communication service provision area into a desired size.

[0096] The base stations CS1 through CS4 wirelessly connect the mobile information terminals MS1 and MS2 described with reference to the first embodiment and the camera-equipped digital mobile phones MS3 and MS4 by W-CDMA (Wideband Code Division Multiple Access) system for example and can communicate mass data at a maximum data transfer rate of 2 Mbps by use of 2 GHz frequency band.

[0097] Because the mobile information terminals MS1 and MS2 and the camera-equipped digital mobile phones MS3 and MS4 can communicate mass data at the high data transfer rate based on W-CDMA system, various kinds of data communication of not only audio talk but also electronic mail transfer, simplified home page browsing, and image transfer can be executed.

[0098] The base stations CS1 through CS4 are connected to a public switched network INW by wired line. The public switched network INW is connected to the Internet ITN, many subscriber wired terminal devices, computer networks, and intranets for example, not shown.

[0099] The public switched network INW is also connected to an access server AS of an Internet service provider. The access server AS is connected to a content server TS owned by the Internet service provider.

[0100] The content server TS is equivalent to the mobile content provider in the first embodiment and provides content such as simplified home pages for example as compact HTML files upon request from subscriber wired terminals, the mobile information terminals MS1 and MS2, and the camera-equipped digital mobile phones MS3 and MS4.

[0101] The Internet ITN is connected to many WWW (World Wide Web) servers WS1 through WS_n. The WWW servers WS1 through WS_n are accessed from the subscriber wired terminals, the mobile information terminals MS1 and MS2 and the camera-equipped digital mobile phones MS3 and MS4 in accordance with the TCP (Transmission Control Protocol)/IP (Internet Protocol) standard.

[0102] With the mobile information terminals MS1 and MS2 and the camera-equipped digital mobile phones MS3 and MS4, the communication with the base stations CS1 through CS4 is made by 2-Mbps simplified transport protocol, while the communication from the base stations CS1 through CS4 to the Internet ITN and the WWW servers WS1 through WS_n is made by TCP/IP.

[0103] A management control unit MCU is connected via the public switched network INW to the subscriber wired terminals, the mobile information terminals MS1 and MS2, and the camera-equipped digital mobile phones MS3 and MS4. In the present second embodiment, this management